The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
04/17/2017

SUBJECT:
A Vulnerability in VMware vCenter Server Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability has been discovered in VMware vCenter Server. VMware vCenter Server, formerly known as VirtualCenter, is the centralized management tool for the vSphere suite. Successful exploitation of this vulnerability could allow for remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE:
There have been no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- vCenter Server versions prior to 6.5c
- vCenter Server versions prior to 6.0U3b

RISK:
Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Low

TECHNICAL SUMMARY:
A vulnerability has been discovered in VMware vCenter Server, which when exploited could allow for remote code execution. This vulnerability occurs due to the use of BlazeDS, a server-based Java remoting and web messaging technology, in order to process AMF3 messages. The issue is present in the Customer Experience Improvement Program (CEIP) plugin and can be exploited during the deserialization of an untrusted Java object. If a customer has opted out of CEIP, the vulnerability is still present and can be exploited. CVE-2017-5641 has been assigned to this vulnerability.

Successful exploitation of this vulnerability could allow for remote code execution in the context of the affected application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Apply appropriate patches provided by VMware to vulnerable systems immediately after appropriate testing.
- If patching is not possible, implement the published workaround for the affected version.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services

REFERENCES:
CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5641

VMware
https://www.vmware.com/security/advisories/VMSA-2017-0007.html
http://kb.vmware.com/kb/2149815
http://kb.vmware.com/kb/2149816

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/